Jurnal Ilmiah Informatika
Volume 1 No. 1 / Desember 2016

IMPLEMENTASI *STATIC* NAT TERHADAP JARINGAN VLAN MENGGUNAKAN IP *DYNAMIC HOST CONFIGURATION PROTOCOL* (DHCP)

Juwanda Natali [1)], Fajrillah [2)], T.M.Diansyah [3)]
[1] Teknik Informatika, STT Harapan Medan
email : juan.nata2412@gmail.com
[2] Teknik Informatika, STT Harapan Medan
email : fajrillahhasballah@gmail.com
[3] Manajemen STIE IBBI Medan
email : dian.22.88@yahoo.com

Abstract

To build a network interconnect Local Area Network (LAN) that will be needed in the form of Virtual groups Local Area Network (LAN). DHCP IP address given by the router to the PC located in the network. NAT (Network Address Translation) is one method that is used as an IP translation to gain entrance into a different network. NAT (Network Address Translation) can allow a host to go into different networks without allowing the host intended to tap into their networks using VLAN With the two different networks into a single switch can be connected. Giving DHCP IP will allow the network administrator to provide the IP address to a PC for IP assigned automatically by the router. An IP host is forwarded in a network with NAT.

***Keyword** : Static nat, VLan, DHCP*

1. PENDAHULUAN

Untuk membangun sebuah interkoneksi jaringan LAN yang besar akan dibutuhkan Virtual dalam membentuk kelompok-kelompok LAN. Apalagi jika ukuran LAN sudah cukup besar, misalkan sebesar kampus atau lebih besar lagi. Dimana masing-masing *host* berada di tempat yang cukup jauh. Akan sangat sulit membuat kelompok berdasarkan kategori tertentu jika lokasi *host* berjauhan. VLAN dapat mengatasi beberapa kesulitan yang tidak dapat diselesaikan oleh LAN tradisional. VLAN dapat digunakan untuk menghubungkan dua *network* yang berbeda dalam satu *switch*.

Dalam merancang jaringan komputer hal yang terpenting untuk diperhatikan adalah IP *Address*. IP *address* dibentuk oleh sekumpulan bilangan biner sepanjang 32 *bit*, yang dibagi atas 4 oktat. Setiap oktat memiliki panjang 8 *bit*. Pemberian alamat IP dapat dilakukan dengan cara *static* dan DHCP, cara *static* dilakukan dengan memasukan alamat IP secara manual. Biasanya cara *static* digunakan untuk pemberian alamat IP terhadap PC yang jumlahnya sedikit. Namun, akan menjadi masalah jika pemberian alamat IP dilakukan dengan cara *static* apabila jumlah PC mencapai 100 *host*. Jika memberikan alamat IP dilakukan secara DHCP tentu akan memberi kemudahan terhadap *admin* jaringan karena setiap PC akan menerima *request* IP *address* secara otomatis dari *router*.

Namun jika pemeberian alamat IP dilakukan secara *static* akan memberikan dampak negatif terhadap *admin* jaringan, sebab memerlukan waktu yang cukup lama untuk pemberian alamat IP satu per satu. Akan tetapi masalah ini dapat diselesaikan dengan memilih pemberian alamat IP menggunakan DHCP. *Dynamic Host Configuration Protocol* (DHCP) adalah salah satu teknik pemberian alamat IP secara otomatis, dimana PC akan meminta IP yang *valid* dari *router*. Konfigurasi DHCP dapat dilakukan pada *router* dengan masuk kedalam CLI (*Command Line Interface*). Dengan DHCP *admin* jaringan tidak memerlukan waktu yang lama untuk memikirkan *host* IP yang akan digunakan karena sudah disediakan oleh *router* secara otomatis. *Admin* jaringan cukup memilih DHCP atau *obtain IP Address Automatically* pada pemberian alamat IP.

Suatu jaringan memiliki arah paket yang datang dari arah yang berubah. Hal ini disebabkan karena *host* memiliki satu alamat IP, tapi semua orang dapat mengakses komputer yang berada di belakang komputer yang memiliki alamat IP yang asli. Dalam keadaan tertentu komunikasi antar *user* dapat terjalin karena proses *routing*. Namun, dalam

proses *routing* komunikasi tidak terjalin jika *network* yang tidak dimasukan. Maka dalam masalah ini diperlukan suatu metode agak *user* dapat masuk kedalam jaringan tanpa proses *routing*. Metode atau teknik yang akan digunakan adalah *static* NAT.

Setiap perusahaan yang memiliki banyak cabang tentunya memilki *server* sebagai penyimpan dan pengolah data perusahaan. Maka tidak semua divisi bisa mengakses *server* tersebut. Untuk itu diperlukan sebuah metode untuk membatasi divisi mana yang boleh mengakses *server* dan divisi mana yang tidak diperbolehkan. NAT *(Network Address Translation)* bekerja mengatur hak akses yang membolehkan suatu IP untuk dilewatkan. Dengan NAT *(Network Address Translation)* tentunya akan membatasi hak akses setiap unit divisi yang ada.

Dalam perancangan suatu jaringan diperlukan sebuah aplikasi yang digunakan sebagai desain *network*. Diantara *software* yang digunakan sebagai *simulator* adalah *Cisco Packet Tracer*. *Packet Tracer* merupakan simulasi *networking* yang dikeluarkan oleh *Cisco System Inc,* yang membantu pengguna dalam proses pembuatan simulasi suatu jaringan sesuai dengan topologi yang telah didesain.

Dalam penelitian perancangan jaringan VLAN disimulasikan dengan *dynamic* NAT. Konfigurasi *dynamic* NAT lebih rumit dan susah dipahami oleh *admin* jaringan. Oleh karena itu penulis ingin mengembangkan jaringan VLAN menggunakan *static* NAT.

2. LANDASAN TEORI

2.1 Jaringan Komputer

Jaringan komputer merupakan kumpulan dari beberapa perangkat yang terkoneksi oleh sebuah media pengiriman data, mekanisme yang memungkinkan perangkat yang terdistribusi dan penggunanya untuk saling berkomunikasi dan berbagi sumber daya.

2.2 VLan

VLAN merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN, hal ini mengakibatkan suatu *network* dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan. Prinsip utama sebuah VLAN adalah, semua *device* yang berada pada satu VLAN berarti berada pada satu *broadcast domain,* Secara umum, beberapa keunggulan yang dimiliki VLAN dibandingkan dengan LAN antara lain yaitu : [4]

1. Performa :Performa jaringan akan meningkat karena paket yang tidak perlu lewat akan diblokir .
2. Fleksibilitas : Desain jaringan akan menjadi lebih fleksibel karena VLAN memungkinkan anggotanya untuk berpindah-pindah lokasi tanpa harus merombak ulang perangkat jaringan.
3. Biaya instalasi yang sedikit : Jika VLAN yang ada ingin diubah, maka tidak diperlukan biaya instalasi maupun perangkat baru.
4. Keamanan : Ketika paket disebar, hanya *user* yang berada dalam satu VLAN yang dapat menerima paket tersebut. *User* di grup yang lain tidak akan melihatnya karena telah tersegmentasi

2.3 DHCP (Dynamic Host Configuration Protocol)

Konfigurasi IP *address* secara DHCP biasa digunakan jika PC yang dibutuhkan dalam *interface* perancangan jaringan skala 30 bahkan sampai 100 PC. [2]

IP *address* dibentuk oleh sekumpulan bilangan biner sepanjang 32 bit, yang dibagi atas 4 bagian. Setiap bagian memiliki panjang 8 bit. IP *address* merupakan identifikasi setiap *host* pada jaringan internet. Artinya tidak boleh ada *host* lain yang tergabung ke internet menggunakan IP *address* yang sama. Contoh IP *address*. [2]

2.4 Network Address Translation (NAT)

NAT (*Network Address Translation*) adalah pengalihan suatu alamat IP ke alamat yang lain. Dan apabila suatu paket dialihkan dengan *Network Address Translation* (NAT) pada suatu link, maka pada saat ada paket kembali dari tujuan maka link ini akan mengingat darimana asal dari paket itu, sehingga komunikasi akan berjalan seperti biasa. Penggunaan utama dari *Network Address Translation* (NAT) adalah untuk membatasi jumlah alamat IP publik suatu organisasi atau perusahaan menggunakan IP publik baik untuk tujuan ekonomi maupun tujuan keamanan. NAT merupakan salah satu *protocol* dalam suatu sistem jaringan, NAT memungkinkan

suatu jaringan dengan IP yang bersifat *private* atau *private* IP yang sifatnya belum teregistrasi di jaringan *internet* untuk mengakses jalur *internet*. [2]

2.5 *Static Nat*

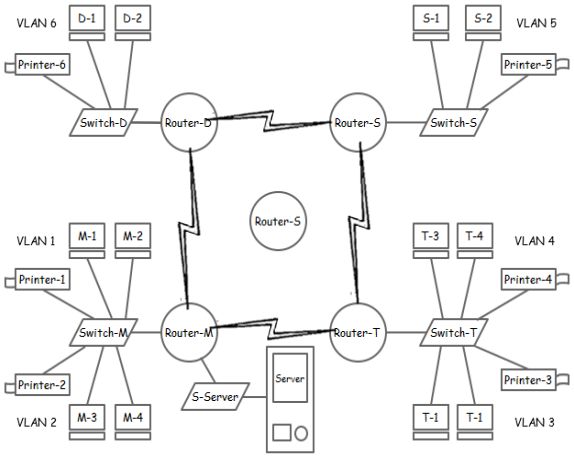
Static NAT atau NAT statis menggunakan *table routing* yang tetap, atau alokasi translasi alamat IP ditetapkan sesuai dengan alamat asal atau *source* ke alamat tujuan atau *destination,* Translasi *Static* terjadi ketika sebuah alamat lokal (*inside*) di petakan ke sebuah alamat *global*/*internet* (*outside*). NAT secara statis akan melakukan *request* atau pengambilan dan pengiriman paket data sesuai dengan aturan yang telah ditabelkan dalam sebuah NAT. [3]

2.6 *Dynamic Nat*

NAT dengan tipe dinamis menggunakan logika *balancing* atau menggunakan logika pengaturan beban, di mana dalam tabelnya sendiri telah ditanamkan logika kemungkinan dan pemecahannya. [2]

3. ANALISIS DAN PERANCANGAN SISTEM

Sebelum melakukan perancangan jaringan VLAN terlebih dahulu membuat konsep jaringan secara logik. Pada desain ini dimisalkan sebuah perusahaan memiliki 4 cabang perusahaan dan masing-masing memiliki satu *router*. *Router-M* kantor pusat, *router*-T untuk Cabang-1, *Router*-D untuk Cabang-2 dan *Router*-S untuk cabang-3. Masing-masing *router* memiliki *Network* VLAN-1: 201.111.10.0, VLAN-2: 202.123.20.0, VLAN-3: 194.234.4.0, VLAN-4: 195.215.5.0, LAN-5: 195.205.15.0, LAN-6: 192.206.6.0. Untuk koneksi *router* pada perancangan ini menggunakan kabel *serial*.

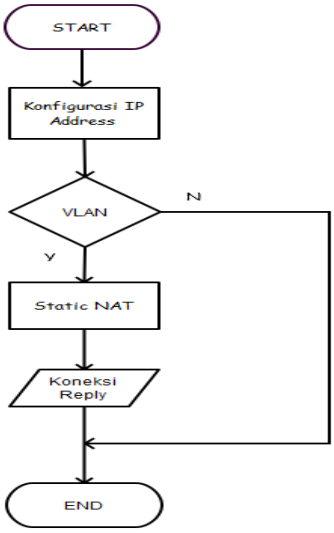


Gambar.1 Desain VLAN

Pada gambar desain VLAN *router* yang digunakan untuk membuktikan peran dari VLAN *Switch* adalah *router*-M dan *router*-T, Dimana dalam *router* tersebut VLAN 1 dan VLAN 2 diberikan dua *network* yang berbeda. IP DHCP akan dibuktikan pada *router*-D dan dan *router*-S, dimana akan dilakukan sebuah konfigurasi agar masing PC yang berada di cabang-2 dan cabang-3 mendeapatkan *request* IP secara otomatis. Untuk pengujian *static* NAT akan dilakukan terhadap PC yang berada di cabang-2, karena PC tersebut berada pada *router* yang berbeda dengan *server*.

3.1 Flowchat

Proses *flowchart* dilakukan untuk menjelaskan diagram alur dari perancangan yang akan dibangun agar lebih mudah untuk dimengerti. Berikut gambar *flowchart* simulasinya:



Gambar 2. *Flowchart* Simulasi

3.2 Konfigurasi DHCP (Dynamic Host Configuration Protocol)

Konfigurasi DHCP dilakukan untuk memberi kemudahan kepada *admin* jaringan dalam pengalamatan IP *address*, *router* mampu memberikan IP secara otomatis tanpa harus memaksa kinerja dari seorang *administrator*. *Router* yang digunakan untuk memberikan IP DHCP adalah *router*-D dan *router*-S. Konfigurasi dilakukan pada *Command Line Interface* (CLI) yang terdapat dalam *router*.

3.3 Konfigurasi VLAN

Konfigurasi VLAN dilakukan untuk menghubungkan *network* yang berbeda tapi

masih dalam satu *switch*. Dalam penelitian ini konfigurasi VLAN dilakukan terhadap *router*-M dan *router*-T.

3.4 Konfigurasi IP Router (Gateway)

IP *gateway* digunakan sebagai penghubung antar *router*. Konfigurasi IP *router* dilakukan agar *router* mengenal IP *address* mana saja yang menjadi *rute* dan IP *network* mana yang akan dikenalkan terhadap *network* lainnya. Konfigurasi IP *router* dilakukan pada *Command Line Interface* (CLI) *router*

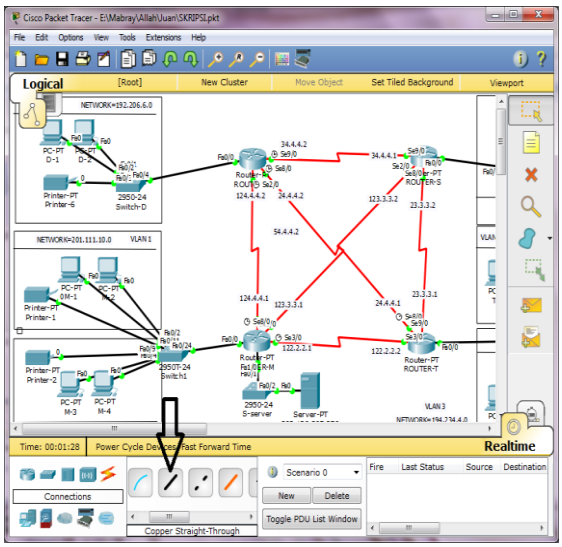
3.5 Analisis Static NAT

NAT (*Network Address Translation*) adalah pengalihan suatu alamat IP ke alamat yang lain, *Static* NAT atau NAT statis menggunakan *table routing* yang tetap, atau alokasi translasi alamat ip ditetapkan sesuai dengan alamat asal atau *source* ke alamat tujuan atau *destination*, sehingga tidak memungkinkan terjadinya pertukaran data dalam suatu alamat IP bila translasi alamat IP nya belum didaftarkan dalam table NAT. Konfigurasi *static* NAT juga dilakukan dengan *command* melalui CLI (*Command Line Interface*).

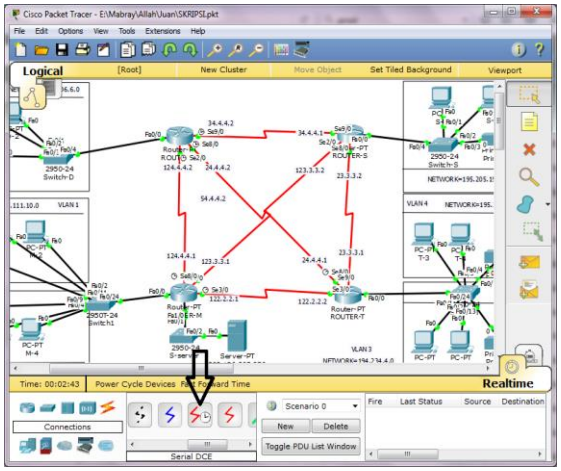
4. HASIL DAN PEMBAHASAN

Pada tahap ini Implementasi static nat terhadap jaringan vlan menggunakan ip dhcp agar dapat dengan mudah memahami cara kerjanya tersebut.

Untuk menghubungkan PC ke PC gunakan kabel koneksi *Straight*. Dan gunakan media kabel *Serial* untuk menghubungkan perangkat *router* ke *router*.



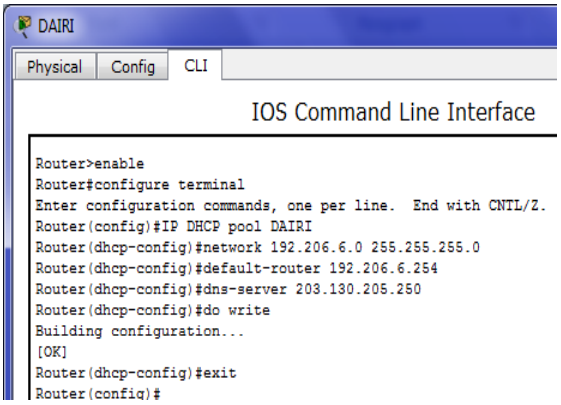
Gambar 3. Media Koneksi *Straight*



Gambar 4. Media Koneksi *Serial*

4.1 Implementasi Konfigurasi IP Address

Setelah desain awal selesai dilakukan, maka selanjutnya pengalamatan IP. Pemberian IP *address* dilakukan dengan cara *DHCP*, akan tetapi untuk jaringan VLAN dilakukan secara manual. Untuk menerima IP DHCP maka lakukan konfigurasi DHCP padar *router*. Berikut konfigurasi IP DHCP:



Gambar 4.3. Konfigurasi IP DHCP *router*-D

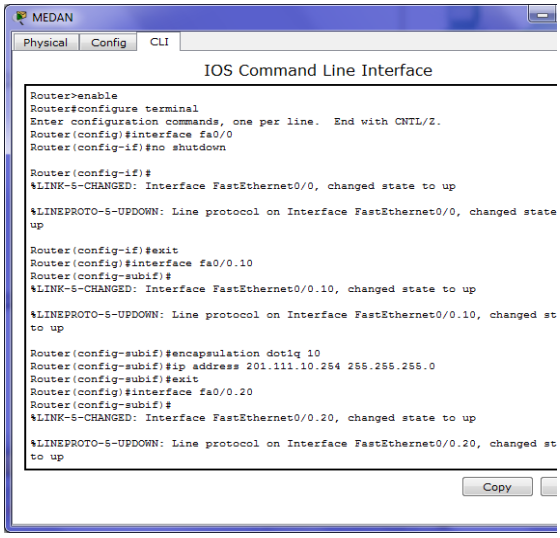
Berdasarkan gambar 4.1 *router*-D diberi nama DHCP DAIRI dan *network* yang akan diberikan adalah 192.206.6.0

4.2 Pemberian IP VLAN

Untuk pemberian IP *address* pada jaringan VLAN maka disediakan dua *network* yang berbeda untuk setiap *switch* nya. *Switch*-M memiliki dua *network* dan *switch*-T juga memiliki dua *network*. Hal ini dilakukan untuk membuktikan apakah VLAN mampu menghubungkan dua jaringan yang berbeda dalam satu *switch*.

VLAN pada *switch*-M dilakukan untuk menghubungkan komunikasi *network* 201.111.10.0 dan *network* 202.123.20.0. Pada dasarnya kedua *network* ini tidak dapat saling

terhubung karena masing-masing *network* memiliki *Net ID* yang berbeda. Maka dibutuhkan sebuah teknik bagaimana menghubungkan dua *network* yang berbeda tapi berada dalam satu *switch.*



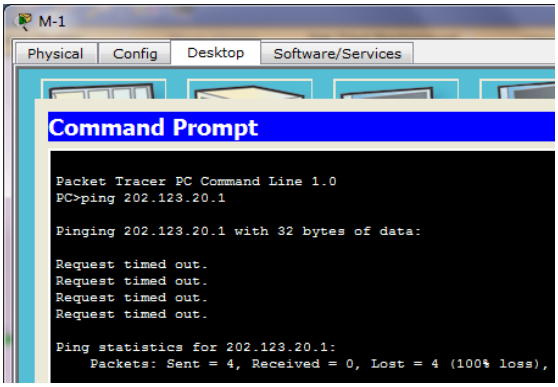
Gambar 5. VLAN *switch*-M

Berdasarkan gambar 4.4 bahwa konfigurasi VLAN *router* dilakukan untuk menggabungkan dua *Net ID* yang berbeda kedalam satu *interface* yang disebut "*interface subif*".

4.3 Pengujian Sebelum VLAN

Pengujian sebelum diterapkan VLAN dilakukan untuk melihat bagaimana koneksi dua *network* yang berbeda dalam satu *switch.*

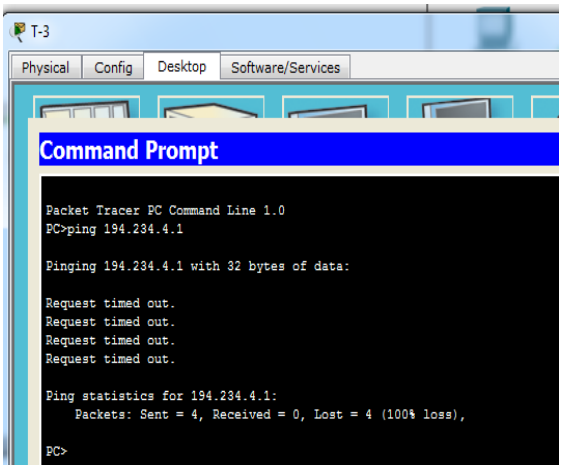
1. PC M-1 terhadap M-3



Gambar 6. PING dari PC M-1 ke M-3 Gagal

Berdasarkan gambar 4.27 bahwa PING dari PC M-1 ke PC M-3 gagal terlihat bahwa tampilan "*Request Time Out*" yang menandakan bahwa koneksi terputus.

2. PC T-3 terhadap T-1



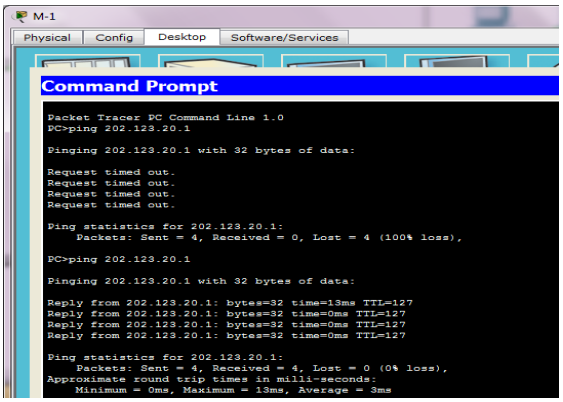
Gambar 7. PING dari PC T-3 ke T-1 Gagal

Berdasarkan gambar 4.28 bahwa PING dari PC T-3 ke PC T-1 juga gagal terlihat bahwa tampilan "*Request Time Out*" yang menandakan bahwa koneksi terputus. Hal ini dikarenak kedua PC berada dalam *network* yang berbeda

4.4 Pengujian Setelah VLAN

Apabila pengujian sebelum menerapkan VLAN koneksi gagal, maka selanjutnya pengujian setelah diterapkannya VLAN. Hal ini dilakukan untuk mengetahui bagaimana peran dari VLAN yang mampu menghubungkan dua *network* yang berbeda tapi berada dalam satu *switch.*

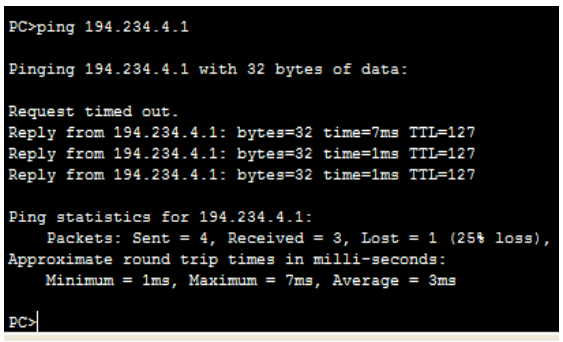
1. PC M-1 terhadap M-3



Gambar 8. PING dari PC M-1 ke M-3 Sukses

Terlihat jelas pada gambar 4.29 bahwa koneksi dari PC M-1 ke PC M-3 dapat terhubung terlihat bahwa tampilan "*Reply TTL=127*" yang menandakan bahwa koneksi terhubung.

2. PC T-3 terhadap T-1

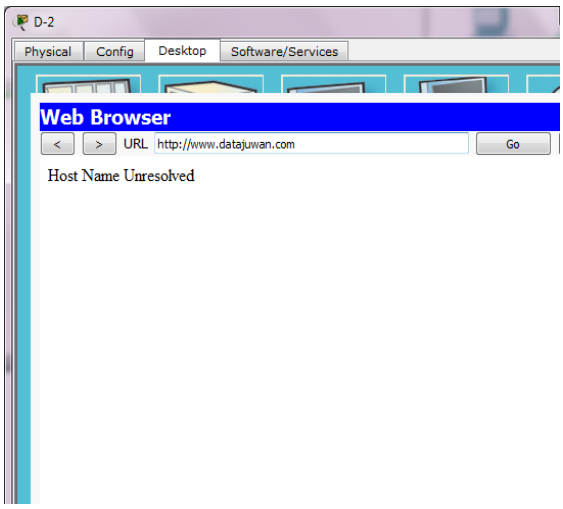


Gambar 9. PING dari PC T-3 ke T-1 Sukses

PING dari PC T-3 ke PC T-1 juga berhasil seperti gambar 9 terlihat bahwa tampilan "*Reply TTL=XXX*" yang menandakan bahwa koneksi terhubung. Hal ini terjadi karena VLAN dapat menghubungkan dua *network* yang berbeda.

4.5 Pengujian Sebelum Static NAT

Pengujian sebelum diterapkannya *static* NAT dilakukan untuk memastikan bahwa koneksi dari PC ke *server* tidak dapat dilakukan. Hal ini terjadi karena *network* PC tidak termasuk dalam tabel *routing*. Pengujian dilakukan menggunakan *web browser* yang terdapat dalam PC.

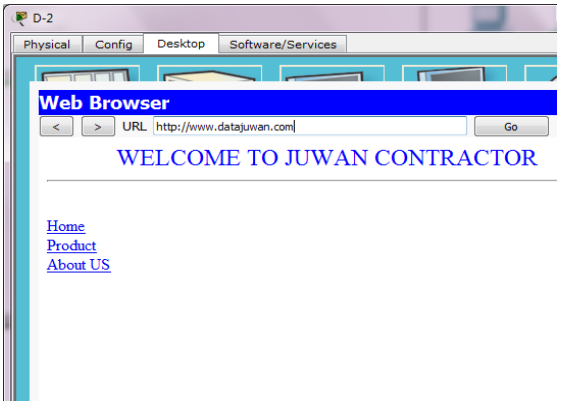


Gambar 10. PING dari PC D-2 ke *Server* Gagal

Berdasarkan gambar 10 pengujian dilakukan melalui "*Web Browser*" dimana sebelum diterapkan NAT maka koneksi PC ke *server* tidak dapat terhubung dibuktikan dengan tampilan "*Host Name Unresolved*".

4.6 Pengujian Setelah Static NAT

Implementasi *static* NAT dilakukan untuk membuktikan koneksi dari PC yang tidak terdaftar oleh *table routing* dapat terhubung ke *server*.



Gambar 11. PING dari PC D-2 ke ke *Server* Sukses

Berdasarkan gambar 4.11 setelah diterapkan *static* NAT maka koneksi dari PC ke *server* dapat terhubung. Hal ini dibuktikan hasil pengujian *web browser* memberikan tampilan sederhana dari *server*.

4.7 Hasil Pengujian

Dari semua hasil pengujian maka dapat dibentuk sebuah hasil pengujian menggunakan *White Box* seperti tabel 1. di bawah ini

Tabel 1. Hasil Pengujian Sebelum VLAN

Router	Nama PC	Koneksi Ke PC	Koneksi Ke *Server*
Router-M	PC M-01	*Request Time Out*	*Request Time Out*
	PC M-02	*Request Time Out*	*Request Time Out*
	PC M-03	*Request Time Out*	*Request Time Out*
	PC M-04	*Request Time Out*	*Request Time Out*
Router-T	PC T-01	*Request Time Out*	*Request Time Out*
	PC T-02	*Request Time Out*	*Request Time Out*
	PC T-03	*Request Time Out*	*Request Time Out*
	PC T-04	*Request Time Out*	*Request Time Out*

Berdasarkan table .1 bahwa sebelum diterapkan VLAN maka koneksi dua *network* yang berbeda akan tetapi dalam *switch* yang sama tidak dapat terjalin. Hal ini dibuktikan dalam tebel pengujian bahwa koneksi ke PC "*Request Time Out"* dan koneksi PC ke *server* juga "*Request Time Out"*.

Tabel 2. Hasil Pengujian Setelah VLAN

Router	Nama PC	Koneksi Ke PC	Koneksi Ke *Server*
Router-M	PC M-01	*Reply*	*Reply*
	PC M-02	*Reply*	*Reply*
	PC M-03	*Reply*	*Reply*
	PC M-04	*Reply*	*Reply*
Router-T	PC T-01	*Reply*	*Request Time Out*
	PC T-02	*Reply*	*Request Time Out*
	PC T-03	*Reply*	*Request Time Out*
	PC T-04	*Reply*	*Request Time Out*

Berdasarkan table 2 bahwa setelah diterapkan VLAN dalam *router*-M dan *router*-T maka koneksi PC ke PC yang berada dalam satu *switch* dapat terhubung. Terlihat hasil pengujian koneksi PC ke PC "*Reply*". Namun koneksi PC ke *server* tidak dapat dilakukan kecuali PC yang berada dalam *router*-M. Hal ini terjadi karena PC berada dalam *router* yang sama dengan *server*.

Untuk mengatasi masalah dua *network* yang berbeda pada satu *switch* maka digunakan teknik VLAN. Dimana VLAN dapat menghubungkan dua *network* yang berbeda berada dalam satu *switch*. VLAN hanya digunakan untuk menghubungkan koneksi PC ke PC bukan PC ke *server*.

Tabel 3. Hasil Pengujian Sebelum *Static* NAT

Router	Nama PC	Koneksi PC *outside*	Koneksi Ke *Server*
Router-M	PC M-01	*Request Time Out*	*Reply*
	PC M-02	*Request Time Out*	*Reply*
	PC M-03	*Request Time Out*	*Reply*
	PC M-04	*Request Time Out*	*Reply*
Router-T	PC T-01	*Request Time Out*	*Request Time Out*
	PC T-02	*Request Time Out*	*Request Time Out*
	PC T-03	*Request Time Out*	*Request Time Out*
	PC T-04	*Request Time Out*	*Request Time Out*
Router-S	PC L-01	*Request Time Out*	*Request Time Out*
	PC T-02	*Request Time Out*	*Request Time Out*
Router-D	B-01	*Request Time Out*	*Request Time Out*
	B-02	*Request Time Out*	*Request Time Out*

Berdasarkan tabel 3. sebelum digunakan NAT maka semua koneksi PC ke *server* terputus kecuali PC *router*-M terlihat tampilan "*Reply*" yang menandakan koneksi terhubung. Hal ini terjadi karena PC berada dalam satu *router* dengan *server*. Untuk menghubungkan koneksi PC ke *server* maka perlu diterapkan *static* NAT

Tabel 4. Hasil Pengujian Setelah *Static* NAT

Router	Nama PC	Koneksi PC *outside*	Koneksi Ke *Server*
Router-M	PC M-01	*Reply*	*Reply*
	PC M-02	*Reply*	*Reply*
	PC M-03	*Reply*	*Reply*
	PC M-04	*Reply*	*Reply*
Router-T	PC T-01	*Request Time Out*	*Request Time Out*
	PC T-02	*Request Time Out*	*Request Time Out*
	PC T-03	*Request Time Out*	*Request Time Out*
	PC T-04	*Request Time Out*	*Request Time Out*
Router-S	PC L-01	*Request Time Out*	*Request Time Out*
	PC T-02	*Request Time Out*	*Request Time Out*
Router-D	B-01	*Reply*	*Reply*
	B-02	*Reply*	*Reply*

Berdasarkan tabel 4 untuk menghubungkan koneksi PC yang tidak dapat terhubung ke *server* maka digunakan *static* NAT. Pada pengujian ini *router* yang akan diberikan NAT adalah *router*-D. Terlihat hasil PING dari PC

ke *server* "*Reply*" yang menandakan komunikasi dapat terjalin dengan baik. Hal ini terjadi karena NAT mampu meneruskan suatu *packet* IP agar dapat terhubung kedalam jaringan yang berbeda.

5. KESIMPULAN

Berdasarkan hasil dari penelitian yang telah dilakukan, maka penulis akan menyimpulkan dari implementasi *Static* NAT pada jaringan VLAN adalah sebagai berikut:*Cisco Packet Tracer* v.6.3 dapat digunakan sebagai *simulator* untuk persiapan *admin* jaringan dalam perancangan jaringan sementara sebelum diterapkan pada dunia nyata,*Virtual Local Area Network* (VLAN) dapat digunakan untuk menghubungkan koneksi dua *network* yang berbeda akan tetapi masih berada dalam *switch* yang sama.*Network Address Translation* (NAT) dapat digunakan sebagai *Translate* IP untuk terhubung pada jaringan yang berbeda tanpa menggunakan *routing.*

6. DAFTAR PUSTAKA

[1] Febri. 2014. *Analisis Kinerja Routing Dinamis Dengan Teknik RIP (Routing Information Protocol) Pada Topologi RING Dalam Jaringan LAN (Local Area Network) Menggunakan Cisco Packet Tracer*. USU Medan.

[2] Trisa M. 2015. *Simulasi Jaringan Frame Relay Menggunakan Metode NAT Dan Dynamic Routing RIP*. STT Harapan, Medan.

[3] Sofana. 2012. *Penerapan Teknik Kriptografi Stream* . Bandung, Informatika.

[4] Karsono. 2013. *Analisis Dan Perancangan Virtual Local Area Network Pada Rumah Sakit Sitanala.* Univ. Esa Unggul, Jakarta.

[5] Yosefina. 2014. *Analisis Dan Perancangan VLAN Pada DISHUBKOMINFO Kabupaten Manggarai Menggunakan Cisco Packet Tracer.* IST AKPRIND Yogyakarta.